Даваажав Сумъяацэрэн

АКТУАЛЬНЫЕ ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В МОНГОЛИИ

Статья посвящена состоянию киберпреступности в Монголии. Дается краткая характеристика киберпреступности на основе анализа статистических данных за последние 10 лет, исследованы способы совершения данного вида преступлений, на основании чего предложены конкретные предложения по борьбе с киберпреступностью в стране.

Ключевые слова: киберпреступление, киберпреступность, преступность в сфере информационных технологий.

Davaagav Cumyaazayrayn

ACTUAL PROBLEMS OF FIGHTING CRIME IN THE INFORMATION TECHNOLOGY FIELD IN MONGOLIA

The article is devoted to cybercrime in Mongolia and the problem of their detection. The author gave a brief overview of cybercrime, based on the analysis of statistical data for the last 10 years, explored ways of committing this type of crimes on the basis of what put forward concrete proposals to combat cybercrime in the country.

Keywords: cybercrime, cybercrime, crime in the field of information technology.

По данным первой половины 2016 г. в Монголии около 2,5 млн пользователей Интернет сети, из них 86,7 % живут в столице Улан-Баторе, 10,3 % в аймачных центрах, 2,9 % в сомонах, а также 59 организаций, имеющих специаль-ные разрешения заниматься деятельностью по предоставлению интернет-услуг и обслуживания [1]. Помимо резкого возрастания интернетпотребления не только через компьютеры, но и с помощью других устройств, имеющих прямой доступ к сети, развиваются виды и способы использования этих достижений в преступных целях.

Многие страны мира ведут борьбу с преступностью в сфере информационных технологий с помощью:

- утдверждения националь-ной политики и стратегии борьбы;
- подготовки компетентных человеческих ресурсов;
- образования инфраструкту-ры охраны;
- утдверждения собственной политики и порядка в каждой организации;
- реализации охраны, осно-ванной на самооценке риска и аудита;образования системы борьбы с киберпреступлениями;
- правовой защиты и охраны;
- повышения общественного знания о киберпреступности [2].

Ни для кого не секрет, что сотрудники правоохранительных органов

по борьбе с киберпреступ-лениями не обладают достаточными знаниями и опытом, не обеспечены технически и методически. К тому же правовое урегулирование отстает от практики. Правоохра-нительные органы сами часто становятся жертвами кибератак и киберпреступлений. Концепция национальной безопасности и “Национальная программа инфор-мационной безопасности” устарели, так как приняты давно.

Правовое урегулирование борьбы с киберпреступлениями недостаточное, не хватает техни-ческих средств и квалифицирован-ных специалистов, способных полу-чить данные из вычислительных устройств и превратить их в дока-зательства. К тому же электронные файлы и их данные не считаются доказательством. Из-за чего раскры-тие киберпреступлений находится на низком уровне. Недостаточное развитие международного сотруд-ничества мешает раскрытию транс-национальных киберпреступлений.

В сетях распространены мошенничество, клевета, вымога-тельство, взлом электронной почты, слежка и т.д.

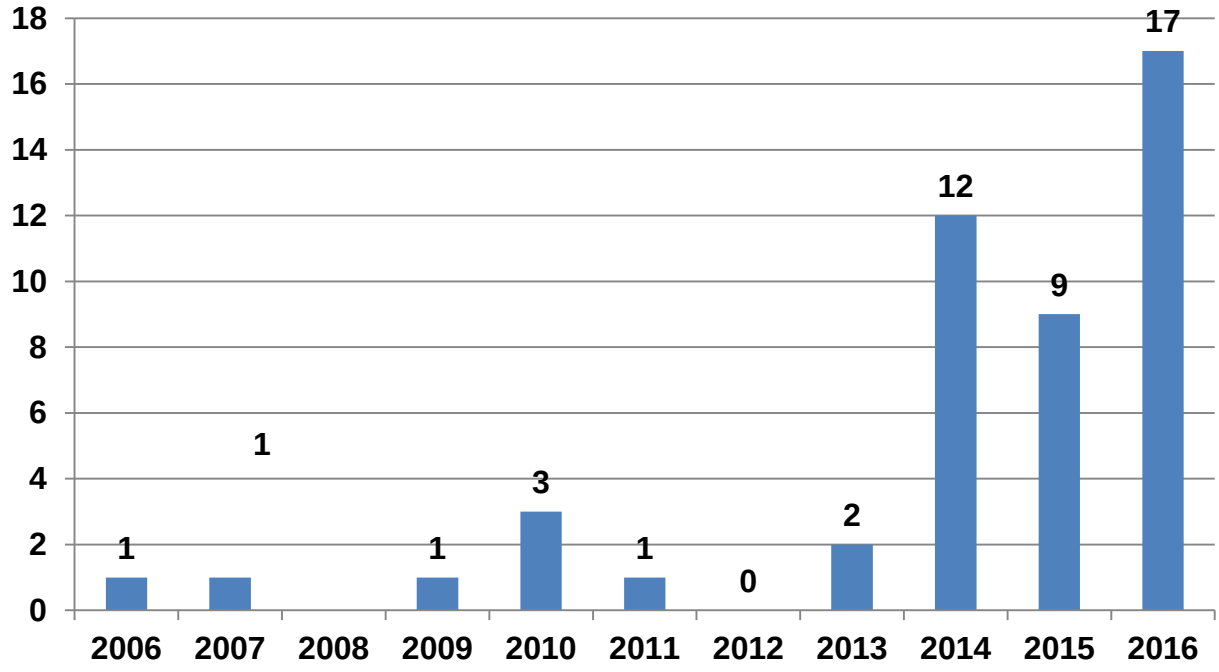

Рис. 1. Динамика роста преступлений против информационной безопасности [4]

Судя по данным последнего десятилетия, число зарегистрированных преступлений по ст. ст. 226–229 УК Монголии увеличивалось в 3–4 раза за последние пять лет (см. рис. 1).

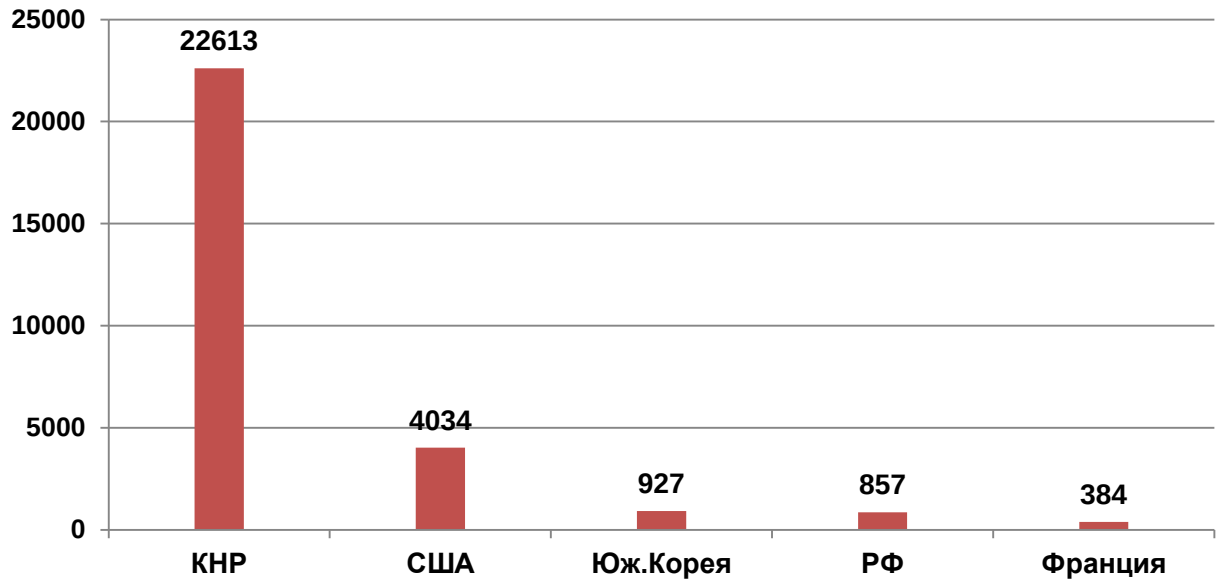

Рис. 2. Количество кибератак из других стран, зарегистрированных в Монголии

Каждый день в Монголии регистрируются сотни кибератак из других государств. Из данных отде-ления кибербезопасности Главного разведывательного управления видно, что в апреле 2016 г. в нашей стране было зарегистрировано 22 613 кибератак из КНР; из США 4 034. Далее идут атаки из Южной Кореи, РФ и Франции (см. рис. 2) [5].

В Монголии распространены такие преступления в сфере инфор-мационных технологий, как мошен-ничество, вымогательство через электронную почту и скимминг. Так, за последние три года в Монголии зарегистрировано 51 мошенничество через электронную почту. Эти преступления причинили ущерб гражданам в сумме 860,572,311 тугриков, хозяйствен-ным организациям – 1,733,475,014 тугриков, всего 2,597,047,325 тугриков [6].

Мошенничество в киберпрост-ранстве происходит через интернет-покупки, рассылку СМС на электронную почту о возможности выиграть деньги в крупном размере, письма о наследстве, о помощи, просьбы прислать счет кредита и т. д.

В Монголии в 2016 г. был организован семинар представителей Фейсбук компании из стран Азиатско-Тихоокеанского региона. На этом семинаре выяснился тот факт, что в Монголии каждый день примерно 950 тыс. человек активно пользуются услугами фейсбук [7]. Кроме того, 5–10 % пользователей,
т. е. около 140 млн человек по всему миру используют фиктивные адреса.

В последнее время преступ-ники, имеющие гражданство таких стран, как Филиппины, Сингапур и Малайзия, используя фальшивые аккаунты, устанавливают связь с нашими гражданами, путем обмена информацией и видеочата собирают личные интимные и секретную информацию граждан, а потом используют их в незаконных сделках. Добытые незаконным путем и

скопированные видеозаписи устанавливают в вебсайты и шантажируют граждан, вымогая крупные суммы денег.

Скимминг считается для нас новым видом киберпреступлений. Скимминг – вид мошенничества, при котором злоумышленники считыва-ют все необходимые данные с магнитной полосы карты и изготавливают ее поддельный аналог [8]. Пин-код они узнают с помощью миникамеры или накладок на клавиатуру, установленных на банкоматах, а затем через дубликат снимают все деньги в пределах лимита выдачи [9]. Данный вид преступлений распространен в развитых странах, и уже зарегист-рирован в Монголии. Например, 4 гражданина КНР установили скимминг-устройство на банкоматах, и за трое суток скопировали информацию с кредитных карт и нанесли ущерб в размере 126,0 млн тугриков.

Начиная с 2012 г., на территории нашей страны выявлен ряд хищений крупных сумм денег с использованием фальшивых кредитных карт из банкоматов коммерческих банков гражданами Украины и Малайзии. Например, граждане Малайзии, использовав фальшивые кредитные карты коммерческих банков Монголии, скупили большую партию товаров в супермаркетах и крупных торговых центрах. Установлено, что преступ-ники хакерским способом внедря-лись в чужие банковские счета и фальшивыми платежными картами расплачивались за покупки [10]. Преступники похитили денежные средства в размере приблизительно 45 млн тугриков. Доказано, что они изготавливают фальшивые банковс-кие кредитные карты не только Монголии, но и других стран. Например, преступники хакерским способом крадут информацию с черных лент банковских кредитных карт таких банков, как “Чейз”, “Ай Ти Эс” и т. д., устанавливают ее на готовые матрицы, изготовленные в Малайзии. Таким образом, вся информация хозяина кредитной карты попадает в руки преступни-ков.

Мировые информационные средства время от времени сообщают о преступных группи-ровках, специализирующихся на преступных деяниях, упомянутых выше. Поэтому международные банки постоянно улучшают и совершенствуют систему контроля, тем самым пресекают возможность мошенничества. Тот факт, что в последнее время эти преступные группировки стали в большом количестве внедряться в нашу страну, возможно связан с несовершенной контрольно-охран-ной системой коммерческих банков Монголии. Это свидетельствует о необходимости коренного улучше-ния охранной и контрольной систе-мы банков.

В ст. ст. 226–229 УК Монголии указывается четыре вида преступ-ных деяний против информацион-ных безопасностей, но не дается понятия киберпреступления.

В соответствии с этим требуется совершенствование законо-дательства, но для этого недос-таточно квалифицированных спе-циалистов в области информа-ционной безопасности, отсутствует внутренняя сеть государственной информации и контроль за интерне-том. В Концепции о Национальной безопасности информационная безопасность

охарактеризована как вид безопасности, но до сих пор в стране не принят основной закон об информационной безопасности.

В высших учебных заведени-ях слабое внимание обращают на подготовку специалистов в области информационной безопасности, а выпускники обладают только общими знаниями, что далеко от современных требований.

Важной проблемой борьбы с киберпреступностью является в первую очередь формирование благоприятной правовой среды, подготовка высококвалифицирован-ных кадров (специалистов), а также обеспечение надлежащих техни-ческих средств и оборудования.

В сотрудничестве с междуна-родным сообществом необходимо разрабатывать программы по проблемам борьбы с киберпреступ-ностью, готовить следователей, создавать лаборатории по исследо-ванию данного вида преступлений.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Комиссия по регулированию коммуникаций Монголии. Статистика потребителей интернета. 2016 г.
2. Цогтбаяр Л. Theoretical and methodical basics of investigation of crimes in cyber environment. Улан-Батор, 2015. С. 150.
3. Уголовный кодекс Монголии. 2002 г.
4. Статистика преступлений (2006–2016 г.) / Национальное полицейс-кое агентство.
5. Отдел кибербезопасности. URL: http://ncsc.gov.mn/index.php?id=135
6. Отчёт отдела по борьбе с киберпреступностью Национального полицейского агентства.
7. Там же.
8. Комсомольская правда. URL: http://www.kp.ru/daily/26555/3027133/
9. Цогтбаяр Л. Theoretical and methodical basics of investigation of crimes in cyber environment. С. 294.
10. Сборник научных статей по материалам международной науч.-практ. конф., посвящ. 20-летию образования Бурятского филиала академии труда и социальных отношений. Улан-Удэ, 2015. С. 468.